TNC-SCAP Use Cases

Paul Bartock

Vulnerability Analysis & Operations Group

Information Assurance Directorate

National Security Agency

24 March 2011

TNC & SCAP Use Cases

- **Comply & Connect**: perform an SCAP based assessment using TNC protocols
- **Pro-active detection & monitoring & quarantine of assets** for un-authorize connections (detection of connection attempts to known bad IPs and domains, via router/ids black list connections)
- **Network sensing and Response:** Security sensors detect suspicious activity and publish this information, which triggers further investigation by A/V or vulnerability or compliance software.

TNC & SCAP Use Cases

Network sensing and Response. Security sensors detect suspicious activity (e.g. traffic sent to known bad IP addresses) and publish this information, which triggers further investigations such as checking caches on other devices to see if they have the same problem. This use case can be implemented through IF-MAP 2.0.

Trends. Administrators get visibility into warning signs by viewing activity on a console. This use case is enabled by IF-MAP 2.0 but nobody has implemented it yet.

TNC & SCAP Use Cases

Rescan for new policy. When an SCAP policy changes, endpoints should be rescanned and their network access modified accordingly. For example, non-compliant endpoints might be quarantined until remediation can be completed.

Information sharing across administrators. The MAP provides a single shared database that allows administrators to have a common view of what's happening on their network. Tricky and interesting issues arise when sharing information across trust boundaries (i.e. from one organization to another). Information may be summarized.

TNC & SCAP Use Cases

Dashboard. Executives and commanders often want a global view of security issues. Which areas of the world are seeing the most attacks? The most compliance or non-compliance? They may also want to drill down to get more information. IF-MAP enables this sort of data to be amassed and exchanged among security systems in a standard way. Thinking is those executives generally view things from a risk perspective. Infections on a critical system are more important than those on a less important one.